UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with Tik Tok Accounts @therealbeeu @thebestxd2021, @user1807845618940

Case No. 1:21MJ321-1

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Daniel BUTTON's TikTok Accounts, namely the following: @therealbeeu; @thebestxd2021; @user1807845618940

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

Evidence of, instrumentalities used in committing, and fruits of the crimes pertaining to violations of 18 U.S.C. Section 2252A, as further described in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2261(A)(1) & (2)	Interstate Stalking / Cyberstalking

The application is based on these facts:

See attached affidavit incorporated by reference herein

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/S/ Zachary M. Neefe
Applicant's signature

Zachary M. Neefe, Special Agent - H.S.I.
Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 8/24/2021 9:41am

Judge's signature

City and state: Durham, North Carol

Joe L. Webster, United States Magistrate Judge
Printed name and title

Certified to be a true and correct copy of the original.
John S. Brubaker, Clerk
U.S. District Court
Middle District of North Carolina
By: _____ Deputy Clerk

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH TIKTOK ACCOUNTS: @therealbeeu @thebestxd2021 @user1807845618940 THAT ARE STORED AT PREMISES CONTROLLED BY TIKTOK INC.	**Case No.** 1:21MJ321-1 **Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Zachary M. Neefe, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of applications pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for information pertaining to certain accounts controlled by TikTok Inc. (hereinafter "TikTok"), an electronic service provider headquartered in Culver City, California. The TikTok accounts to be searched are the following: @therealbeeu, @thebestxd2021, and @user1807845618940 (herein after "Target Accounts"), as further described below and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require TikTok to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. Based on my training, experience, and the investigation the facts summarized in this affidavit, I submit there is probable cause to believe that:

a. **DANIEL MILLER BUTTON**, has committed violations of 18 U.S.C. §§ 2261(A)(1) & (2), Interstate Stalking & Cyberstalking and 18 U.S.C. § 2252A(a)(5)(B), Possession of Child Pornography (collectively hereinafter, the "**Target Offenses**"); and,

b. a search of the **TARGET ACCOUNTS** will reveal evidence, instrumentalities, contraband, and/or fruits of the **Target Offenses**, as further described in Attachment B.

AGENT BACKGROUND

3. I have been employed as a Special Agent ("SA") of the U.S. Department of Homeland Security ("DHS"), Homeland Security Investigations ("HSI") since February of 2020 and am currently assigned to the Winston-Salem, North Carolina, Office of the Resident Agent in Charge. Prior to working with HSI, I was a detective and federal task force officer at the Alamance County Sheriff's Office in North Carolina where I specialized in child exploitation and sexual abuse investigations.

4. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training facilitated by the Internet Crimes Against Children ("ICAC") Task Force, at the National Cybercrimes Center ("C3"), and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography, child exploitation, and sex trafficking and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. My training through C3 and the ICAC Task Force has included undercover chats for child exploitation cases, peer-to-peer file sharing of child pornography, online ads pertaining to enticement of children, and training specific to the Bittorrent file sharing technology. Moreover,

I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. § 2252A (relating to child pornography) as well as 18 U.S.C. § 2261(A) (relating to interstate and cyber stalking as alleged here).

5. I have personally participated in the investigation described herein and have witnessed some of the facts and circumstances described herein. I have also received information from other federal and local law enforcement and intelligence officials relating to this investigation. The information set forth in this affidavit is based on my own observations and review of documents, or reliable information provided to me by other law enforcement personnel. Because this affidavit is being prepared for the limited purpose of securing the requested search warrants, I have not set forth all facts known to me about this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of the **Target Offenses**, as further described in Attachment B, will be within the electronic data of the **TARGET ACCOUNTS**, as further described in Attachment A.

SUMMARY CONCERNING PERSONS WHO POSSESS AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND THE INTERNET RELATES TO THE POSSESSION, RECEIPT AND DISTRIBUTION OF CHILD PORNOGRAPHY

6. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the internet to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or cellphone, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence,

or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer to Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

7. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers, smartphones and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers, smartphones and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a computer (via a USB cable) or connect with a computer via Bluetooth, and transfer data files from one digital device to another. Some "smartphone" users can and do create, communicate, upload, and

download child pornography, and communicate with children to coerce them or entice them to produce child pornography or perform sexual acts, by using internet based social media or electronic service providers like Instagram, Snapchat, or Apple (and many others).

d. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo, and Google, LLC, Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers and is occasionally retained by the providers after the user deletes the data from their account.

f. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store,

maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

g. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

h. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over a terabyte of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

i. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and on the evidence of known Internet-based communications further described below, there exists a fair probability that evidence regarding the production, distribution, receipt and possession of child pornography will be found in the **TARGET ACCOUNTS** notwithstanding the passage of time.

PROBABLE CAUSE

*Victim A.B. Reports that **BUTTON** Has Been Stalking Her Online for Over a Year*

8. On May 26, 2021, the Winston-Salem Police Department ("WSPD") received a report of online stalking activity. WSPD Officer M.J. Konrad documented the activity under WSPD Case Number: 2128516. The victim, A.B., stated that she was an online content creator

with accounts present on Tik Tok, Instagram, Twitter[1], and other video-centric social media platforms. In that capacity, A.B., who goes by the online alias of "PeachyFizz" across multiple websites/platforms, generated cosplay videos which mainly focused on Korean pop artists (aka K-Pop). A.B. explained that cosplay was the practice of dressing up as a character from a movie, book, or video game. In this capacity, A.B. stated she had a massive following of 1.4 million people and 51.9 million likes on her videos under the Tik Tok account associated with her cosplay.

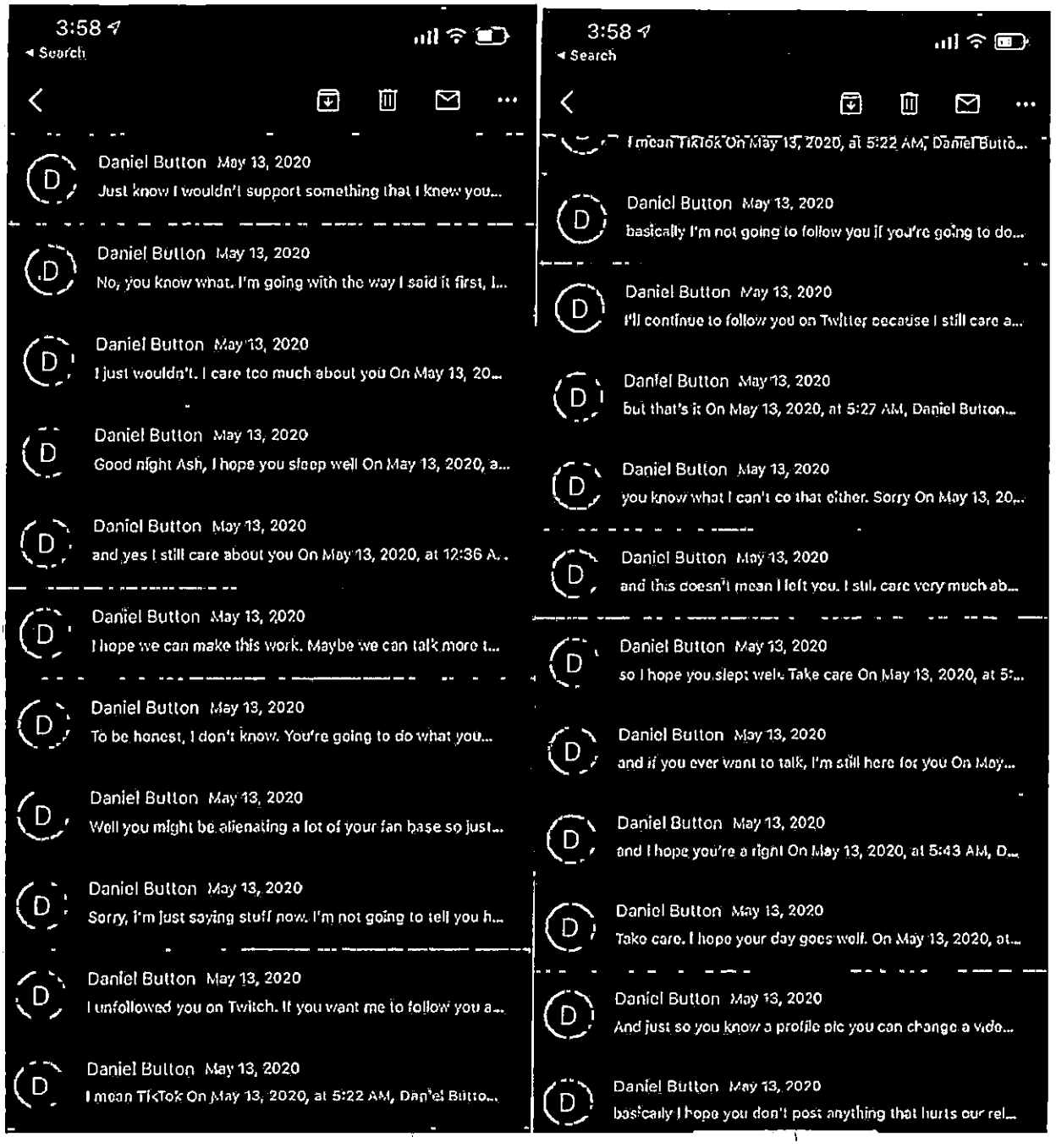
9. A.B. reported to the WSPD that beginning in or around April 2020, an enamored fan, later identified by A.B. as Daniel Miller **BUTTON**, purchased an expensive (approximately $100.00) pair of cosplay shoes for her off an Amazon Wishlist linked to her various social media accounts. A.B. stated she thanked **BUTTON**, as it was her practice to do so for large-item donors.

10. Shortly, thereafter, **BUTTON** began engaging in what A.B. described as stalking behavior, which, A.B. reported, continued for more than a year.[2] Specifically, from April 2020 until A.B. filed her initial report with WSPD on May 26, 2021, A.B. alleged that **BUTTON** had sent her hundreds of messages via her various social media channels. The messages A.B. received were sometimes affectionate, sometimes rambling, and sometimes threatening. For example, below is a screenshot of emails that A.B. received from **BUTTON** through the email account danielbutton01@gmail.com, all on a single day (May 13, 2020):

(*see next page*)

[1] Tik Tok, Instagram, and Twitter are internet based social media platforms where users can post content, comment on other's content, and direct message one another.

[2] A.B. was a minor when **BUTTON** started communicating with her. She turned 18 a few months ago, in April 2021.



Emails from danilebutton001@gmail.com to A.B. on May 13, 2020

11. A.B. stated that she began to be fearful of **BUTTON** when he threatened her, sent messages to her that were vulgar in nature, or that insinuated that she and **BUTTON** were in an exclusive dating relationship (A.B. clarified repeatedly with law enforcement that she has never been in any type of relationship with **BUTTON**). A.B. explained that **BUTTON** sent her Twitter

messages of pornography in which **BUTTON** tagged A.B.'s online accounts, pornographic links or images, and messages that included direct and indirect threats of violence. For example, on May 17, 2021, **BUTTON** sent A.B. social media messages (included below) in which **BUTTON** accused A.B. of having a sexual relationship with his father, an individual A.B. did not know and had never met, and then told A.B. she would "burn at the stake" and "spend the rest of eternity in hell.. I'll make sure of it [sic]."

Instagram messages from "nofriendsdaniel" to A.B. on May 17-19, 2021

12. A.B. reached a breaking point when, on May 21, 2021, **BUTTON** sent A.B. a photo of a bloody, dismembered female corpse (below) with the message, "can't wait for this to be you."

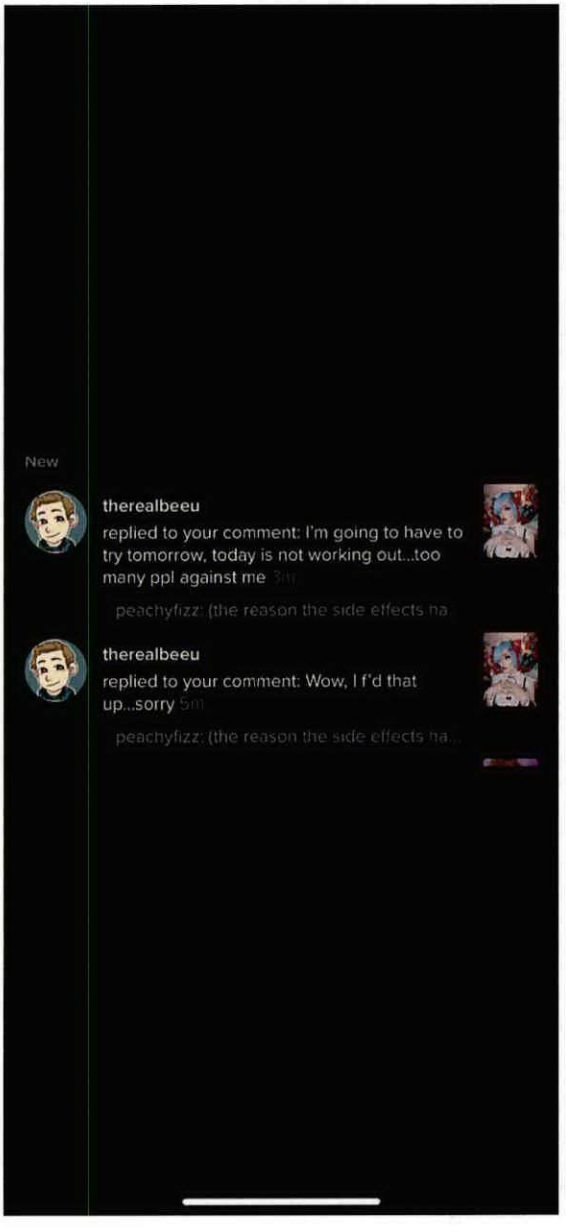
*Photo **BUTTON** sent to A.B. on May 21, 2021 with message "can't wait for this to be you"*

13. Five days later, on May 26, 2021, A.B. reported **BUTTON** to the WSPD A.B. explained that she had attempted to block **BUTTON** and his various usernames from contacting her via social media and repeatedly and explicitly asked him to stop contacting her. **BUTTON** refused. He continued to contact A.B. despite her efforts by establishing new social media names/accounts and email addresses that A.B. had not yet blocked. For example, on or about March 4, 2021, **BUTTON** sent the victim the following message:

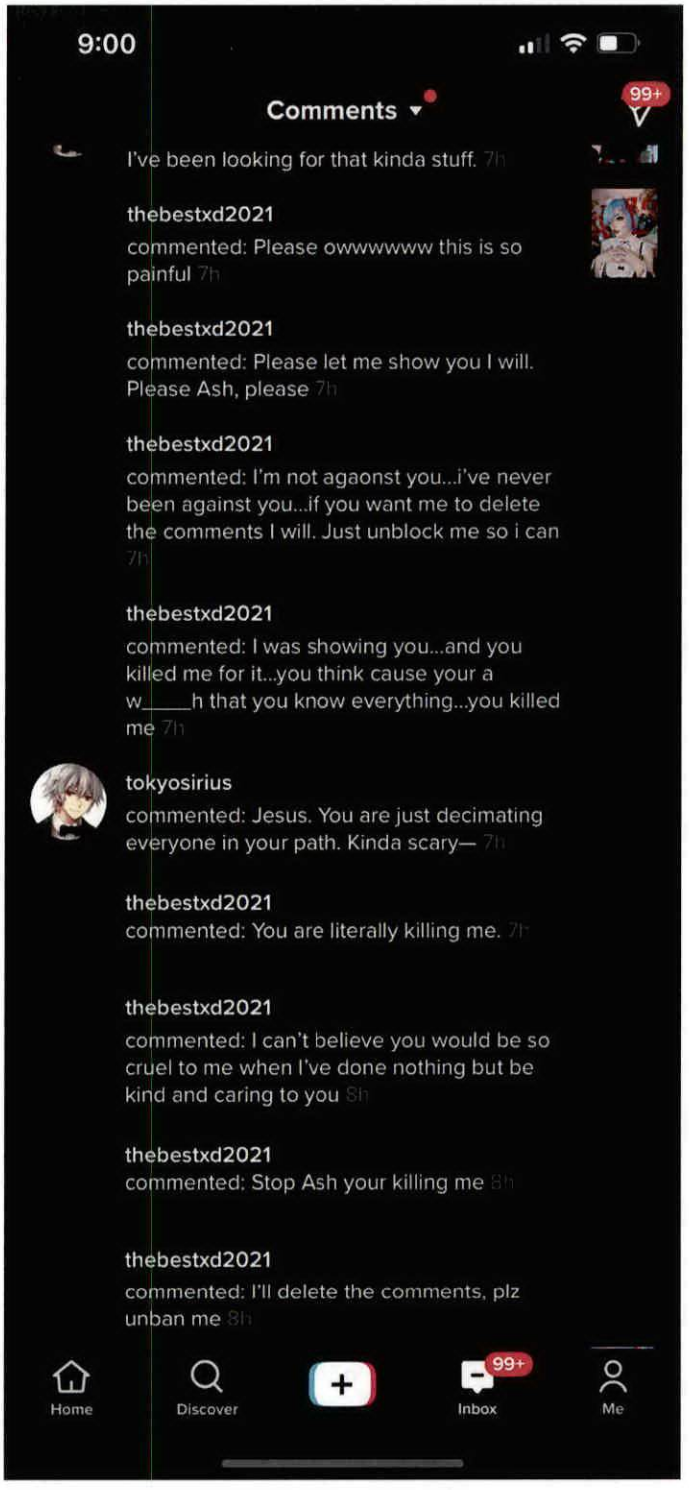
> "Please stop blocking me Ash…I just wanted you to know I'd fuck you if that's what you really wanted. Like, hello, if you wanted to have sex then yeah, I'd 'hit' that . . . . Sweetheart you are a straight up b-i-t-c-h . . . Oh and wouldn't you love to end my rein on earth. I bet your so happy scoring all those bonus points knowing you're going against God and you'll be rewarded in the life and afterlife by all these demons who have chosen to go against me. You don't care about all the suffering going on in the world. You're fucking encouraging it. I know your thoughts Ash, I know you have sworn to kill Jesus Christ upon his return. It's too bad you didn't have faith in me and instead relied on demons . . . Whatever at least you live in your

glorious cum filled heaven. You clearly didn't want me there anymore. Fine, then fuck you."

14. With regards to the specific **TARGET ACCOUNTS** associated with TikTok, I confirmed that communication did appear to exist between **BUTTON** and A.B. The following are screenshots containing the TikTok accounts named in this search warrant:



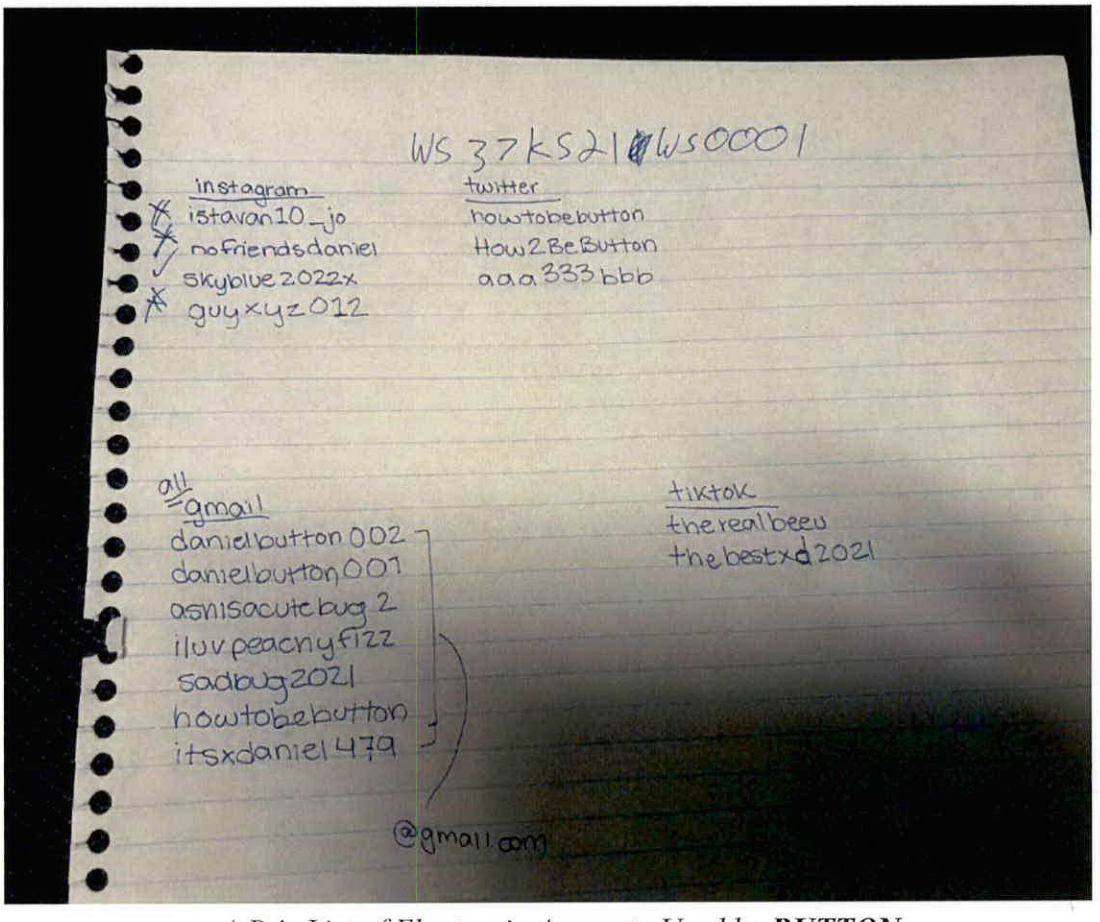
@therealbeeu TikTok Account as identified by victim A.B.



@thebestxd2021 TikTok Account as identified by victim A.B.[3]

[3] The last named TikTok account (@user1807845618940) will be discussed further & quoted later within this affidavit in order to keep the fact pattern as chronological as possible.

15. A.B. kept track of the different electronic platforms (including the associated **TARGET ACCOUNTS**) and account names **BUTTON** used to harass her and provided the information she had collected to law enforcement (see photo below).



A.B.'s List of Electronic Accounts Used by ***BUTTON***

16. To preserve the messages she received, A.B. printed out numerous stacks of screen shots form her electronic devices that she gave to WSPD and later reviewed with federal agents.[4]

[4] On July 14, 2021, members of Homeland Security Investigations' ("HSI") conducted a "forensic" interview with A.B. during which a third-party interviewer spoke with A.B. in a recorded setting and law enforcement was able to confirm the various accounts that **BUTTON** had used. Additionally, law enforcement collected content and metadata associated with many of the communications. As set forth below, on or about June 24, 2021, law enforcement officers seized from **BUTTON** pursuant to his arrest a cell phone assigned call number (216) 212-2959. As of the time of this affidavit, law enforcement is attempting to ascertain whether this same number was utilized to setup the various accounts used by **BUTTON** for communication with the victim.

Throughout her interviews, A.B. stressed that the messages were unsolicited by her and that she considered them to be a legitimate threat to her safety and wellbeing.

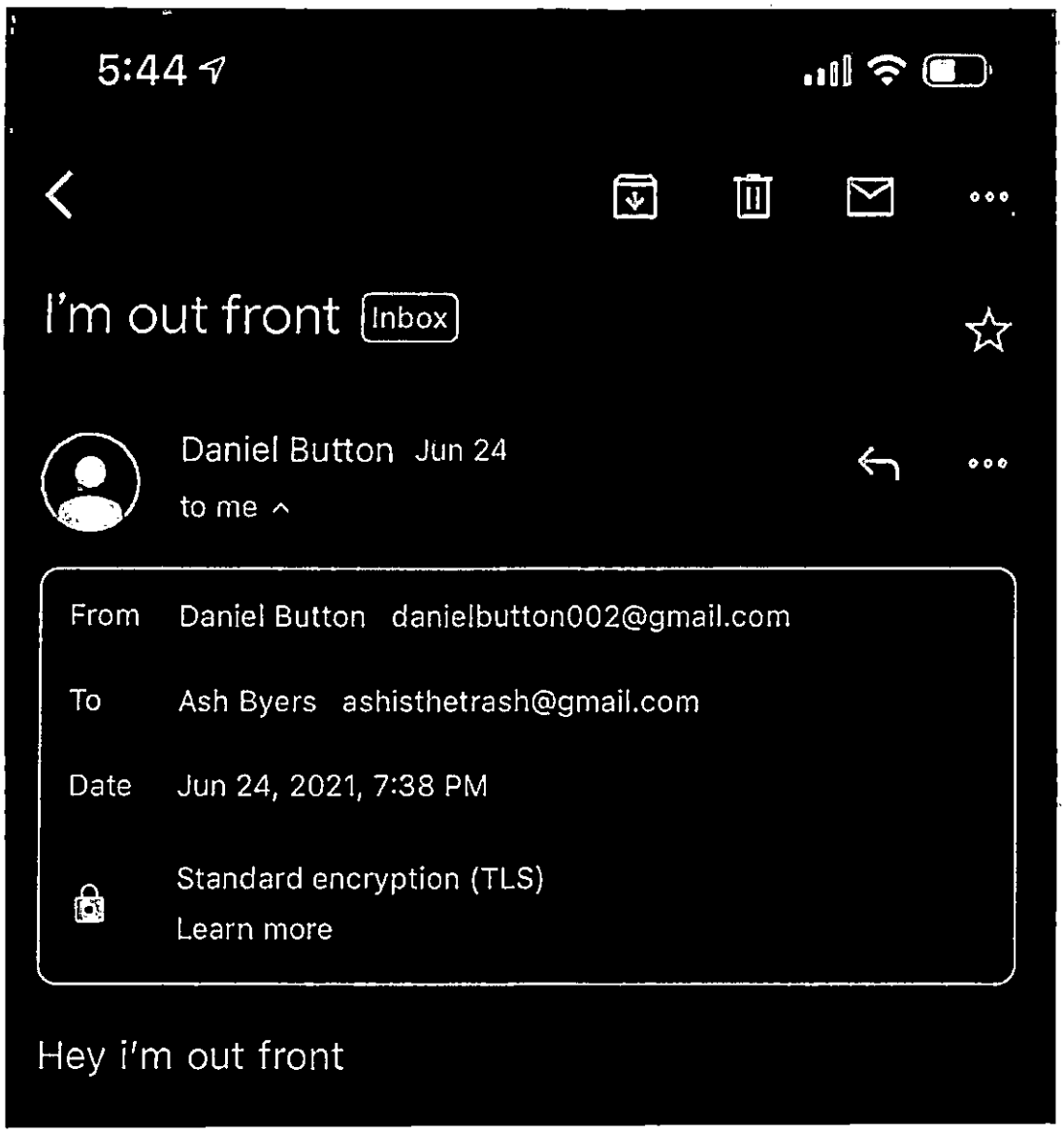
***BUTTON** Travels to North Carolina and Appears at the Victim's Home*

17. Following A.B.'s initial police report on May 26, 2021, WSPD referred the incident to their investigations division for follow up, but in the meantime **BUTTON's** harassment continued.

18. On or about June 24, 2021, **BUTTON**, who lives in Bethesda, Maryland, showed up at A.B. home in North Carolina. A doorbell camera captured footage of **BUTTON** as he approached the home and rang the doorbell. The images captured by the doorbell camera (provided below) match known photos of **BUTTON** obtained from booking photos during **BUTTON**'s arrest on the same date.

*Doorbell footage from June 24, 2021, of **BUTTON** at the front door of A.B.'s residence*

19. In addition, **BUTTON** emailed the victim contemporaneously with his in-person appearance at her home in North Carolina:



Email from danielbutton002@gmail.com to A.B. on June.24, 2021

20. A.B.'s family members immediately called 9-1-1 and **BUTTON** was taken into custody by WSPD a short time later. During a subsequent recorded interview with WSPD, after waiving his *Miranda* rights, **BUTTON** admitted that he had rented a car and driven from Maryland to North Carolina for the express purpose of meeting A.B. **BUTTON** explained that he had wanted to "talk" to the victim at a coffee shop or other public place and said she could bring a friend or

relative if she desired.[5] **BUTTON** further admitted that he had been communicating with A.B. through her social media accounts.

21. Following his arrest, on June 24, 2021, **BUTTON** was charged by state warrant with misdemeanor charges for stalking and communicating threats. *See State of North Carolina v. Daniel Miller Button*, District Court for Forsyth County, North Carolina, 21-CR-055701. In connection with those charges, on June 30, 2021, the BUTTON was released subject to certain conditions memorialized in a release order. The release order stated, among other provisions, that the "The defendant shall have NO CONTACT with the prosecuting witness, [A.B.]."[6]

22. The next day, on July 1, 2021, after BUTTON attempted to contact A.B. indirectly by communicating with one of her friends, the court amended the conditions of pre-trial release to clarify that "The defendant shall have NO DIRECT OR INDIRECT CONTACT with [A.B.]"

23. Homeland Security Investigations ("HSI") Task Force Officers ("TFOs") and Special Agents ("SAs"), including me, became involved in this investigation in July 2021 in order to facilitate examination of two digital devices—a cell phone and a laptop—seized from **BUTTON** at the time of his arrest for which WSPD later obtained search warrants.

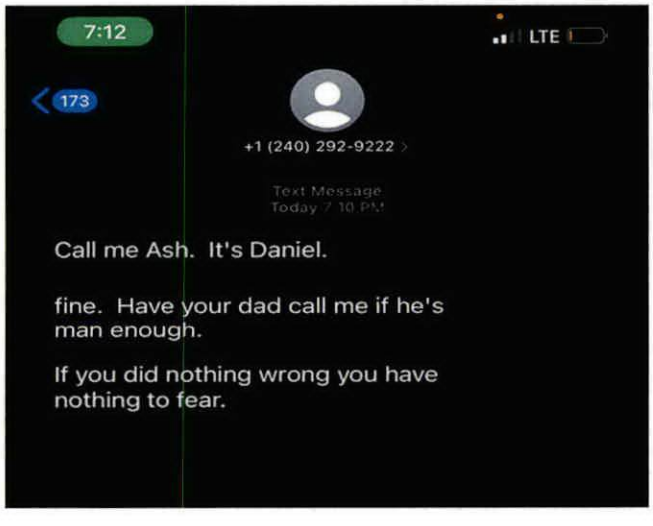
24. On July 26, 2021, HSI's victim coordinator learned that A.B. was continuing to receive unsolicited contact from **BUTTON**. Specifically, on July 25, 2021, I reviewed a Tik Tok

[5] At the time of his arrest, **BUTTON** was wearing a torn hoodie with a bloody white shirt underneath. During his post-*Miranda* interview, **BUTTON** insinuated that he didn't care about the blood on the hoodie because it gave off a vibe of carefree/rebellious spirit. **BUTTON** also stated the blood came from known nosebleed issues and was not worn to intimidate A.B.

[6] After posting bail, **BUTTON** returned to Maryland where he became involved on or about June 30, 2021, in an altercation with his parents and was subsequently involuntarily hospitalized in Montgomery County for a short time. According to the Montgomery County Police Report issued in connection with the altercation, **BUTTON** told his father, "i'm going to fucking come hunt you down," because **BUTTON** "believe[d] his father was in North Carolina not to bail him out but to see a 16 year old [sic] Tik Tok star that Daniel was just arrested for stalking."

message in which Tik Tok user @user1807845618940 stated the following (summarized for brevity): "Hi Ash, you are more beautiful than you'll ever know. every day, minute, and sec I don't see your video is like 10000 knives through my body . . . [WSPD] officer konrad is a good guy. he'll protect you when I'm there. my lawyers are saying you are charging me with assault attempted murder stalking . . . ." I am aware that WSPD Officer Michael Konrad was one of the officers who arrested and interviewed **BUTTON** on June 24, 2021. Based on the identification of Konrad and the reference in the message to pending charges, I believe this message was sent by **BUTTON** (and A.B. believed so as well).

25. Further, on July 26, 2021, A.B. received three text messages from phone number (240) 292-9222 in which the sender—who identified himself as "Daniel"—instructed A.B. to call him. The second message stated "fine. Have your dad call me if he's man enough." The third message said, "If you did nothing wrong you have nothing to fear." A.B. explained she did not give **BUTTON** her number and was unsure how he had obtained her contact information.



Text messages A.B. received on July 26, 2021

26. On July 27, 2021, at approximately 3:32 in the morning, **BUTTON** left a voicemail on A.B.'s cellphone from a new phone or number (as noted above, WSPD seized a phone seized

from **BUTTON** during his initial arrest in North Carolina on June 24, 2021). In the message, the caller identified himself as "Daniel" and repeatedly asked A.B. to talk.

27. Following this violation of the local no contact order, on July 27, 2021, a federal magistrate judge in the Middle District of North Carolina issued a criminal complaint and arrest warrant for BUTTON based on two counts of cyber and interstate stalking in violation of 18 U.S.C. § 2261(A)(1) and (2).

28. Overnight, prior to **BUTTON's** early morning arrest on July 28, 2021, A.B. received approximately ten additional voicemails from the new cell phone number, (240) 292-9222, and a number that was blocked.

***BUTTON's** Arrest on Federal Charges and Connection to his residence (previous "SUBJECT PREMISES" from Search Warrant in Maryland)*

29. On July 28, 2021, special agents from HSI's Baltimore, Maryland office arrested **BUTTON** on the federal arrest warrant outside of his apartment and advised **BUTTON** of his *Miranda* rights. Present during the arrest were HSI Special Agents as well as HSI Task Force officers and representatives from the Montgomery County Police Department. Prior to execution of the arrest warrant, all participating law enforcement officers were provided with a booking photograph from **BUTTON's** arrest in North Carolina on June 24, 2021.

30. During a search incident to arrest, HSI agents located in **BUTTON's** pants pockets a Maryland driver's license with BUTTON's photograph and identifiers; a bank card in the name "Daniel Button" and two black-colored cellular phones. Before he was transported to the custody of the U.S. Marshal Service at the federal courthouse in Greenbelt, Maryland, **BUTTON** gave HSI agents permission to enter his apartment, which he said was number 414, and to leave his personal property (the license, bank card, and cell phones) inside. BUTTON's property was returned to his apartment and the door locked to secure it.

31. Subsequently, during his transport to Greenbelt, while the vehicle was completely silent, **BUTTON** stated in sum and substance, "This is about Ashley, I hope she is doing ok, I tried to reach out to her and her parents and didn't get a response." BUTTON then asked the HSI special agents in the car if they had spoken to A.B., and then said "This is about [A.B.], it's not that bad." HSI agents then reiterated that **BUTTON** again that he has the right to remain silent and did not have to speak to them about his case. **BUTTON** acknowledged that he understood.

32. HSI agents later spoke with representatives of the property management company responsible for **BUTTON's** apartment complex and the representatives confirmed that **BUTTON** was a resident.[7]

*Suspected Child Pornography on **BUTTON's** Phone*

33. On or about August 3, 2021, I reviewed the contents of **BUTTON's** phone (seized by the WSPD and subsequently turned over to HSI for phone forensics) with another HSI Computer Forensic Analyst/Special Agent ("SA Brant"). During this review, I observed two suspected child pornography files that were stored in **BUTTON's** phone under the following filepath: iPhone/mobile/Containers/Data/Application/com.comcsoft.iZip/Documents/Samples v3/Samples v3. SA Brant stated that, based on his training and experience, this filepath was indicative of storage for an unknown app on **BUTTON's** phone.

34. The two videos are as follows:

a. 08032021_1.mp4: a video 46 seconds in length depicting a prepubescent female positioned on a bed with an unknown-aged male. Both subjects were fully nude. As the

[7] During his arrest, **BUTTON** stated he was staying with a roommate. However, the property manager for the apartment complex in which **BUTTON**'s apartment is located was not aware of any residents in the unit other than **BUTTON**.

video progressed, the unknown-aged male received oral/penile sex from the juvenile, with the sex acts then progressing to penile/anal intercourse.

b. 08032021_2.mp4: a video 19 seconds in length depicting a prepubescent female in a bathroom with an adult white male. The minor was positioned directly in front of the adult male, who appeared naked from at least the waist down. As the video progressed, the adult male received oral/penile sex from the juvenile.

MANNER OF SEARCHING COMPUTER SYSTEMS

35. As described here and in Attachment B, this application seeks permission to search for records in any form that they may be found in the **TARGET ACCOUNTS**, including electronic records stored on electronic devices. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

36. I submit that if electronic data is found in the **TARGET ACCOUNTS**, there is probable cause to believe evidence of the crimes set forth in this affidavit will be located, for the reasons set forth above as well as at the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files

downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

37. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for forensic, electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **TARGET ACCOUNTS** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration

information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and

events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer

behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

38. Based on my training and experience, I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

39. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always

possible to search computer equipment and storage devices for data for several reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, website, or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises or a vehicle; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear

that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

40. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

41. Additionally, based on past investigations involving digital devices (such as cellphones), I am aware that there are significant collections of data that are potentially relevant, irrelevant, exculpatory, and/or incriminating on any digital device. Even in the case of a relatively new cellphone, initial account setup, installed telephone number, applications, storage programs, photos, videos, and other data on the device could prove to be vital to the involved investigation. Linked cloud accounts or other online identifiers could also prove vital to identifying additional off-device premises for service of new legal process for those premises' digital contents based on the newly-identified account being associated with the digital data found inside TARGET ACCOUNTS. In an age of increased interconnectivity and cloud-based computing technologies, it is possible that this service of process for the **TARGET ACCOUNTS** will only serve to identify and confirm additional electronic service providers where ultimately, the data resides off-site and will require another search warrant for proper access.

42. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

43. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that Daniel Miller **BUTTON** has committed these offenses. Furthermore, there is probable cause to believe that the contraband, property, evidence,

fruits, and instrumentalities of these offenses, more fully described in Attachment B, are located at the location described in Attachment A. I respectfully request that this Court issue a search warrant for the location described in Attachment A authorizing the seizure and search of the items described in Attachment B.

/S/ Zachary M. Neefe
Zachary M. Neefe
Special Agent
Homeland Security Investigations

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) on this 24th day of August, 2021 at 9:41am.

Honorable Joe L. Webster
United States Magistrate Judge

Certified to be a true and
correct copy of the original.
John S. Brubaker, Clerk
U.S. District Court
Middle District of North Carolina
By: _____
Deputy Clerk
Date: August 24, 2021

ATTACHMENT A

(Property to be Searched)

Electronic data contained within Daniel BUTTON's TikTok Accounts, namely, the following:

- @therealbeeu
- @thebestxd2021
- @user1807845618940

ATTACHMENT B
(Items to be Seized)

I. Information to be disclosed by Tik Tok (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. Subscriber Information, as defined in TikTok's Law Enforcement Guidelines as containing, at a minimum, the following information: TikTok username, Email address(es), Phone number(s), Account creation date, IP address at account creation, Device information;

b. Log-in / log-out data, as defined in TikTok's Law Enforcement Guidelines as containing IP address logs from account activity within the **TARGET ACCOUNTS**;

c. Interaction data, as defined in TikTok's Law Enforcement Guidelines as containing non-content IP address logs for interactions as well as video creation time / dates associated with the **TARGET ACCOUNTS**;

d. Content data, as defined in TikTok's Law Enforcement Guidelines as containing video content, comments, and direct message content.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

a. All information described above in Section I which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § 2261(A)(1) & (2), Interstate Stalking & Cyberstalking, and 18 U.S.C. § 2252A(a)(5)(B), Possession of Child Pornography

b. Records and information constituting, referencing, or revealing child pornography, as defined in 18 U.S.C. § 2256(8), and child erotica;

c. Records and information constituting, reference, or revealing cyberstalking and/or interstate stalking within the meaning of 18 U.S.C. §2261A

d. Records and information referencing or revealing the use or ownership of the TARGET ACCOUNTS, or any variation thereof;

e. Records and information referencing or revealing the trafficking, advertising, or possession of child pornography, to include the identity of the individuals involved;

f. Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved;

g. Records and information referencing or revealing communication or interaction of an illicit sexual nature with minors, to include the identity of the individuals involved;

h. Records and information referencing or revealing communication or interaction with "PeachyFizz"

i. Records and information referencing or revealing participation in groups or the use of services that are known to be used to facilitate the trafficking of child pornography;

j. Records and information referencing or revealing the use of remote computing services such as email, cloud storage, or online social media services;

k. For all items described in this section, all metadata, transaction information, storage structure, and other data revealing how the items were created, edited, deleted, viewed, or otherwise interacted with;

l. Records and information revealing or referencing information about the device(s) used to access the account;

m. Records and information revealing or referencing the identity of the individual who created and used the account; and

n. Identity of accounts linked by cookies.

With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, to minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

e. "Surveying" various file directories and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files).

f. "Opening" or cursorily reading the first few pages of such files in order to determine their precise contents.

g. "Scanning" storage areas to discover and possible recover recently deleted files.

h. "Scanning" storage areas for deliberately hidden files.

i. Performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

2. If after performing these procedures, the directories, files or storage areas do not reveal evidence of child pornography or other criminal activity, the further search of that particular directory, file or storage area, shall cease.

3. With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

4. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the

court. The investigative team may continue to review any information not segregated as potentially privileged.